UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/775,797	02/10/2004	Ramarathnam Venkatesan	MS307073.01/MSFTP588US	9675

27195 7590 07/30/2008

AMIN. TUROCY & CALVIN, LLP
24TH FLOOR, NATIONAL CITY CENTER
1900 EAST NINTH STREET
CLEVELAND, OH 44114

EXAMINER	
TRAORE, FATOUMATA	

ART UNIT	PAPER NUMBER
2136	

NOTIFICATION DATE	DELIVERY MODE
07/30/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docket1@thepatentattorneys.com
hholmes@thepatentattorneys.com
lpasterchek@thepatentattorneys.com

Office Action Summary	Application No.	Applicant(s)	
	10/775,797	VENKATESAN ET AL.	
	Examiner	Art Unit	
	FATOUMATA TRAORE	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 April 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4,6-18 and 20-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 2, 4, 6-18 and 20-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response of the amendment filed April 8, 2008. Claims 3, 5 and 19 have been cancelled. Claims 1, 20, 28, 33-35 have been cancelled. Claims 1, 2, 4, 6-18 and 20-35 are pending and have been considered below.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. The previous 101 rejection however regarding 1-19 have been withdrawn in light of the amendment to claims 1-19. However, claims 20-27 and 33 are not statutory. Claim 20 is drawn to components, which the applicant has defined in the specification (page 7, lines 4-15) to encompass a program, an executable, etc). A computer program is not a series of steps or acts and this is not a process. A computer program is not a physical article or object and as such is not a machine Or manufacture. A computer program is not a combination of substances and therefore not a compilation of matter. Thus, a computer program by itself does not fall within any of the four categories of invention. Therefore, Claim 1 and dependant claims 20-27 and 33-35 are not statutory.

Response to Arguments

4. Applicant has substantially amended the claims. In particular, Applicant has amended the independent claims to recite, "a tracing component that determines whether a user accessing the first code is a valid user via a unique watermark associated with a particular user and embedded in the first code, wherein f the

watermark does not correlate to an authorized user, access is denied." In particular, Applicant argued that "Manferdelli et al does not disclose a system that utilizes a tracing component to determine whether a user accessing the code is a valid user" and that "a unique watermark associated with a particular user is embedded therein." Applicant contended that the watermark of Venkatsesan et al is merely associated with a pre-defined function of the code" and that Venkatsesan et al does not teach "a unique watermark embedded within the first code and associated with a particular user." Applicant's arguments with respect to the claims have been considered but are moot in view of the new ground(s) of rejection. However, it should be pointed that the association of the watermark with a particular user and granting access based on the watermark are taught in the prior art, as will be used below in the rejection.

Muratani (US 2004/0153941)discloses a code generating method and unit thereof, code detecting method and unit thereof, and watermark embedding unit and watermark detecting unit, wherein a first code is transformed into a second code and a watermark is embedded into the first code (abstract, [0080]). According to Muratani, the watermark is associated with a user ([0080], [0081], [0137], and [0309]). Muratani also discloses verifying or tracing component for determining whether a user is a valid used based on the watermark ([0080], [0081], [0082], and [0324]). Muratani further discloses the new code as a protective wrapping of the first code such that an attack on the first code would appear as k/a noise ([004]). See also figures 6A and 6B.

Alattar et al [US 2005/0 1356561 discloses an authentication of physical and electronic media objects using digital watermarks, wherein a watermark is embedded into a signal (abstract, fig 1, item 106). Alattar et al also discloses a watermark reader (116) for extracting or reading the watermark (abstract) and comparing the watermark for authentication purpose as to determine whether a user is a valid user (abstract), [0045]. Alattar et al also discloses associating the watermark with a particular user (abstract), wherein authentication is based on the watermark associated with the user (abstract, [0042] to [0044]).

Brundage et al [US 2007/0016790] discloses an identification document and related method, wherein a watermark is embedded into a document (fig. 5 and [0015]). The watermark, according to Brlindage et al, is associated with a user and authentication is provided based on the watermark (abstract, [0057]). Brundage et al also discloses verifying or tracing the watermark so as to determine whether a user is a valid user (abstract, [0027], [0050]).

Moskowitz (US 2008/0046742) discloses optimization methods for the insertion, protection, and detection of digital watermarks in digital data. According to Moskowitz, a watermark is embedded into a content signal (abstract, [0007], [0013]). Also, Moskowitz discloses detecting an verifying/tracing the watermark (abstract, [0034], associating the watermark with a particular user ([0030], [0031], [00371). Moskowitz further discloses using a second code as a protective wrapper for a first code against an attack on the first code [0050].

Kim (US 2002/013 8730) discloses an apparatus and method for inserting and detecting watermark based on stochastic model, wherein a watermark is embedded into a signal (abstract) and the watermark is associated with a unique user.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-2, 4, 6, 11-12, 15-16, 20, 28, 30-31 and 33-35 rejected under 35 U.S.C. 102(e) as being anticipated by if pass stuff(US 2008/0046742).

Claims 1, 20, 28 and 33-35: Moskowitz discloses a system that facilitates efficient code construction, comprising:

i. A processor for executing the following components (*processor for identifying an area of the digital signal) (paragraphs [0011], [0034]):*

ii. A component that receives a first code(a receiver to receiver digital signal) (*paragraph [0034])* designed in a noise model, the first code comprises algorithms utilized to correct noise errors with high probability, the first code is intended to refer to encoded data as well as error

detection codes and includes a linear code(*paragraphs [0021]-[0022], [0050]*); and

iii. A transformation component that transforms the first code to a new code that has essentially same length parameters as the first code but is hidden to a computationally bounded adversary, the transformation component utilizes a random number generator to perform algebraic transformations on data utilizing the first code to generate the new code, and the transformation component hides the first code via randomizing data that employs the first code thereby not enabling the computationally bounded adversary to determine a location of critical bits to attack (*paragraphs [0011], [0047]*),

iv. wherein the new code acts as a protective wrapping of the first code, such that an attack on the new code by the computationally bounded adversary would appear as a noise attack on the first code *(It also helps that the error is random, and so over time, appears as white noise, which is relatively unobtrusive)(paragraph [0050]),* as the attack would be randomly distributed across the first code and not concentrated on a particular location within the first code, this allows the first code to act as it was designed to and utilize(*paragraphs [0047], [0050])* .;

v. wherein the first code designed in the noise model utilizes the algorithms to correct the noise errors with a high success rate (*paragraph [1016]);*

vi. A decoder that determines the first code from the new code, the decoder accesses algorithms utilized by the transformation component to decode the new code and determine the first cod (*paragraphs [0024], [0026]);* and

vii. A tracing component that determines whether a user accessing the first code is a valid user via a unique watermark associated with a particular user and embedded in the first code wherein if the watermark does not correlate to an authorized user, access is denied (paragraphs [0030], [0031], 0034], [0037]).

Claim 2: Moskowitz discloses a system that facilitates efficient code construction as in claim 1 above, and Moskowitz further discloses that the new code appears random to the computationally bounded adversary *(It also helps that the error is random, and so over time, appears as white noise, which is relatively unobtrusive) (paragraph [0080], [0094]).*

Claim 4: Moskowitz discloses a system that facilitates efficient code construction as in claim 1 above, and Moskowitz further discloses that the transformation component comprises a pseudo-random number generator that facilitates transforming the first code into the new code (*creation of a pseudorandom key*)(*paragraph [0109]).*

Claim 6: Moskowitz discloses a system that facilitates efficient code construction as in claim 1 above, and Moskowitz further discloses that the decoder comprising

a checking component that determines whether the first code has been corrupted (*paragraph [0048]).*

Claim 11 : Moskowitz discloses a system to be that facilitates efficient code construction as in claims 1 and 28 above, and Moskowitz further discloses wherein the first code is generated based at least in part on a sequence of messages *(random bit errors are error bits occurring in a random manner, whereas burst errors may exist over large sequences of the binary data comprising a digitized signal) (paragraph [0085]).*

Claims 12 and 31 Moskowitz discloses a system and method that facilitates efficient code construction as in claim 11 and 28 above, and Moskowitz further discloses that the decoder knowing the sequence of messages (*paragraph [0024]).*

Claims 15 and 30: Moskowitz discloses a system and method that facilitates efficient code construction as in claims 11 and 28 above, and Moskowitz further discloses that the transformation component embeds information relating to the sequence of messages into the new code (*paragraphs [0061], [0067]).*

Claim 16: Moskowitz discloses a system that facilitates efficient code construction as in claim 15 above, and Moskowitz further discloses the first code has a length of nl, and the information relating to the sequence of messages embedded in nl locations in the new code(*paragraphs [0061], [0067]*).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 7-8, 25 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moskowitz (US 2008/0046742) in view of Cox (US 6,275,965).

Claim 7: Moskowitz discloses a system as in claim 6 above, but does not explicitly disclose that the checking component utilizing a checking function h" Zn {0,1}, where E is a finite alphabet that defines a family of codes and n is a length parameter for E. However, Cox et al discloses a system for efficient error detection and correction, which further discloses that the checking component utilizing a checking function h" Zn {0,1}, where E is a finite alphabet that defines a family of codes and n is a length parameter for E *(column 11, line 66 to column 12, line 40)*. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the teaching of Moskowitz such to use checking function. One would have been motivated to do so in order to provide for enhancing the error detection and correction capability obtained when a plurality of data byte strings or vectors are interleaved and encoded in a two-level, block-formatted linear code using codeword (sub block) and block-level redundancy (column 2, line 64 to column 3, line 2).

Claim 8: Moskowitz discloses a system as in claim 6 above, but does not

explicitly disclose that the checking component outputting a vector, the first code being corrupted when the vector is a non-zero vector . However, Cox et al discloses a system for efficient error detection and correction, which further discloses that the checking component outputting a vector, the first code being corrupted when the vector is a non-zero vector (*column 8, lines 23-38, column 9, lines 9-25; Fig. 5*). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the teaching of Moskowitz such to compute a nonzero vector output. One would have been motivated to do so in order to provide for enhancing the error detection and correction capability obtained when a plurality of data byte strings or vectors are interleaved and encoded in a two-level, block-formatted linear code using codeword (sub block) and block-level redundancy (column 2, line 64 to column 3, line 2).

Claims 25 and 29: Moskowitz discloses a system and a method as in claims 20 and 28 above, but does not explicitly disclose that comprising decoding the message, wherein the message is decoded at least in part by solving a minimum vertex cover problem. However, Cox et al discloses a system for efficient error detection and correction, which further discloses that comprising decoding the message, wherein the message is decoded at least in part by solving a minimum vertex cover problem(column 3, line 50 to column 4, line 15). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the teaching of Moskowitz such as to solve a vertex

problem. One would have been motivated to do so in order to increase data integrity and system security.

9. Claims 9 and10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moskowitz (US 2008/0046742) in view of Guruswami (Foundations of Computer Science, 2001, Proceedings, 42nd IEEE Symposium, Pages: 658- 667, ISBN: 0-7695-1116-3).

Claim 9 Moskowitz discloses a system that facilitates efficient code construction as in claim 1 above, but does not explicitly disclose that the decoder utilizes a unique decoding function, Guruswami discloses a similar system, which further discloses a decoder utilizing a unique decoding function (*we further consider the list decoding version) (introduction and section 5*). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the teaching of Moskowitz discloses a system that facilitates efficient code construction as in claim 1 above such as to include a unique decoding function. One would have been motivated to do so in order to increase data integrity and system security.

Claim 10: Moskowitz discloses a system that facilitates efficient code construction as in claim 1 above , but does not explicitly disclosed that the decoder utilizes a list decoding function g, Guruswami discloses a similar system, which further discloses a decoder utilizing a list decoding function *(we further consider the list decoding version) (introduction and section 3*). Therefore, it

would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the teaching of Moskowitz such as to include a list decoding function. One would have been motivated to do so in order to increase data and system security.

10. Claims 13-14, 17-18 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moskowitz (US 2008/0046742) in view of Venkatsesan et al (US 6,829,710).

Claims 13, 17 and 32: Moskowitz discloses a system and method that facilitates efficient code construction as in claims 12, 16 and 31 above, and Moskwitz further discloses a pseudo random number generator(*paragraph [0109]*), but does not explicitly discloses that the pseudo random number generator generates two pseudo random numbers a and b, each n number of bits, based upon a position within the sequence of one of the messages, and further generates a random permutation o- that permutes the n bits. However, Venkatesan et al discloses a technique for producing, through watermarking, which further discloses that the pseudo random number generator generates two pseudo random numbers a and b, each n number of bits, based upon a position within the sequence of one of the messages, and generating a random permutation σ that permutes the n bits(*Fig. 9A, item 936*).Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the teaching of Moskowitz such to generate two random

numbers based on desistance One would have been motivated to do so in order to securely watermark any executable (column 4, lines 4-49).

Claim 14: Moskowitz and Venkatesan disclose a system that facilitates efficient code construction as in claim 13 above, and Venkatesan et al further discloses the transformation component sends a randomized code word to the decoder, the randomized code word having the form a x ~(f(mi))+ b, where f is an encoding function, m is a message, i is the position of the message within the sequence, and x is a bitwise multiplication operator(column 8, lines 34-43). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify teaching of Moskowitz such to generate two random numbers. One would have been motivated to do so in order to securely watermark any executable (column 4, lines 4-49).

Claim 18: Moskowitz and Venkatesan et al disclose a system as in claim 17 above, and Venkatesan et al further discloses that an encoder sending the new code to the decoder, the new code having embedded therein the seed (*column 8, lines 10-35*). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the teaching of Moskowitz such to generate two random numbers. One would have been motivated to do so in order to securely watermark any executable (column 4, lines 4-49).

11. Claims 21-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moskowitz (US 2008/0046742) in view of Bohnke (US 6,557,139).

Claim 21:Moskowitz discloses a system as in claim 20 above, while neither of them explicitly discloses that the message is encoded with a minimum relative distance. However, Bohnke discloses a similar system, which further discloses an encoding component that encodes a message and creates a code word, the encoding component encodes the message with a code that has a minimum relative distance. Epsilon. And rate 1-.kappa..epsilon. for some constant .kappa.>1. (In FIG. 3, a block diagram of an encoding structure according to the present invention is shown, which comprises a data input means, a checksum generator, a frame formatter and a turbo encoder. The data input means receives serially arranged data bits, e. g. in data frames consisting of N data bits, d.sub.0, d.sub.1, . . . d.sub.N-1. (Column 5, lines 50-55). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the teaching of Moskowitz such as to include such an encoder. One would have been motivated to do so in order to increase data and system security.

Claim 22: Moskowitz and Bohnke disclose a system as in claim 21 above, and Bohnke further discloses a component that utilizes the encoded message and divides the encoded message into a number of blocks B, the B blocks being of substantially similar size (Fig.1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the teaching of Moskowitz such as to use block encryption. One would have been motivated to do so in order to increase data and system security.

Claim 23: Moskowitz and Bohnke disclose a system as in claim 22 above, and Bohnke further discloses the plurality of blocks encoded using (n, k, n – k + 1) Reed-Solomon code, where n is a resulting size of the encoded blocks and k is a size of the blocks prior to encoding (column 7, lines 25-35). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the teaching of Moskowitz such as to use the Reed-Solomon code. One would have been motivated to do so in order to increase data and system security.

12. Claims 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Moskowitz (US 2008/0046742) in view of Bohnke (US 6,557,139) in further view of Guruswami (Foundations of Computer Science, 2001, Proceedings, 42nd IEEE Symposium, Pages: 658- 667, ISBN: 0-7695-1116-3).

Claim 24:Moskowitz and Bohnke disclose a system as in claim 23 above. While neither reference explicitly discloses that the code hiding module comprising a bipartite expander graph with a number of edges being substantially similar to Bn, and symbols within the B blocks are randomly assigned an edge within the bipartite expander graph, Guruswami discloses a similar system, which further discloses an expander graph with a number of edges being substantially similar to Bn, and symbols within the B blocks are randomly assigned an edge within the bipartite expander graph(the construction employ expander graphs, which facilitate efficient decoding algorithms through various forms of voting

procedures) (introduction and section 4). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined teaching of Moskowitz and Bohnke such as to include an expander graph. One would have been motivated to do so in order to increase data and system security.

13. Claims 26 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moskowitz (US 2008/0046742) in view of Tian et al (US 6,714,683).

Claim 26:Moskowitz discloses a system as in claim 20 above, but does not explicitly disclose that the system comprises a synchronization component that synchronizes the code generator with the decoder. Tian et al discloses wavelet based feature modulation watermarks, which further discloses, which further discloses a synchronization component that synchronizes the code generator with the decoder(Column 1, line 65 o column 2, line 5). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the teaching of Moskowitz such as to include such to synchronize the decoder. One would have been motivated to do so in order to increase data and system security.

Claim 27:Moskowitz discloses a system as in claim 20 above, but does not explicitly disclose the code hiding module embeds synchronization information into the second code. Tian et al discloses wavelet based feature modulation watermarks, which further discloses, which further discloses that the code hiding

module embeds synchronization information into the second code (column 4, lines 38-60). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the teaching of Moskowitz such as to include such to synchronize the decoder. One would have been motivated to do so in order to increase data and system security..

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

FT

Wednesday, July 23, 2008

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2136